HWG | HARRIS, WILTSHIRE & GRANNIS LLP

September 24, 2019

Ex Parte

Ms. Marlene H. Dortch
Secretary
Federal Communications Commission
445 12th Street, SW
Washington, DC 20554

Re: *Modernizing the E-rate Program for Schools and Libraries (WC Docket No. 13-184)*

Dear Ms. Dortch:

The record overwhelmingly and unanimously supports the inclusion of modern network security on the Funding Year 2020 Eligible Services List ("ESL").[1] Aruba, a Hewlett Packard Enterprise Company, hopes that the Commission and Wireline Competition Bureau can act in time for network security to be eligible in Funding Year 2020.[2] This technology is urgently needed to address the cybersecurity crisis schools and libraries currently face.[3] Towards that goal, Aruba offers the following definition of network security for consideration.

Aruba submits that network security includes the following:

---

1 Letter from Julie A. Veach, Counsel to Aruba, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 13-184 (filed Sept. 6, 2019) (citing, among other submissions, Reply Comments of the Council of Chief State School Officers at 1, WC Docket No. 13-184 (filed Sept. 3, 2019); Reply Comments of the American Library Association at 3-4, WC Docket No. 13-184 (filed Sept. 3, 2019); and Initial Comments of the State E-rate Coordinators' Alliance, WC Docket No. 13-184 (filed Sept. 3. 2019)).

2 Ideally the Commission or Bureau would release the ESL at least 60 days before the opening of the Funding Year 2020 application window as required by 47 C.F.R. § 54.502(d). For good cause, the Commission has previously waived the requirement that the ESL be released 60 days before the opening of the application filing window. *See, e.g.*, *Schools and Libraries Universal Service Support Mechanism*, Report and Order and Further Notice of Proposed Rulemaking, 25 FCC Rcd. 6562, 6566, 6583 & n.161 (2009) (waiving the 60-day rule and citing three prior instances of waiving the rule).

3 *See, e.g.*, Maggie Miller, *Cyberattacks find easy target in nation's schools*, THE HILL (Aug. 8, 2019), https://thehill.com/policy/cybersecurity/456780-cyberattacks-find-easy-target-in-nations-schools ("School districts across the country are increasingly becoming a major target of malicious cyberattacks . . . .").

- **Advanced Network Security Hardware and Software** components secure network access, devices, and users; enhance network integrity and visibility; and prevent unauthorized access to network resources and internet access.[4] This includes, among other things, authentication portals and systems to verify that a device has permission to access the network, receives appropriate access rights, and meets minimum security requirements, such as running an up-to-date operating system and appropriate anti-virus software, before allowing access to network resources.

Advanced network security systems are critical for preventing unauthorized access to sensitive information and administrative-level settings and for preventing insecure devices from potentially infecting network assets. These systems also allow network administrators to identify and cut off network access for compromised devices to limit the impact of an incident.

- **Intrusion Detection/Intrusion Prevention** systems work in addition to firewalls to monitor network activity and detect internal and external threats to a network. They monitor network traffic for malicious activity that may interrupt or gain control over network applications and devices, reporting any threats to system administrators and blocking malicious behavior.[5]

Intrusion prevention systems are essential for preventing attacks such as denial of service, distributed denial of service, ransomware, and other exploits and viruses. These attacks risk significant downtime and compromising sensitive information.[6]

- **Data protection** components ensure the continued operation of eligible equipment by protecting equipment and computer files from environmental and security hazards. Data protection includes encryption of information in transit and at rest, backup and recovery systems for restoring operations after an incident, and appropriate data retention systems. These systems ensure that only necessary information is retained, that access is restricted to the appropriate persons, and that access to data can be readily restored if lost or otherwise rendered unavailable due to ransomware or another attack.[7]

---

4 *See, e.g.*, Reply Comments of CoSN, AASA and ASBO, K-12 Cybersecurity Cost Report at 9, WC Docket No. 13-184 (filed Sept. 3, 2019) (advocating for "[e]nhance[d] user access security and end point device security" as one component "to offset the high-risk cybersecurity threats and high[] cost of mitigating them") ("CoSN Cybersecurity Report").

5 *See, e.g.*, *id.* at 3 (explaining that "[a] 'standard' firewall across the technology industry" offers, among other things, advanced threat protection, DDoS mitigation, and intrusion detection and protection); Comments of EducationSuperHighway at 7, WC Docket No. 13-184 (filed Aug. 16, 2019) (explaining that intrusion detection and prevention systems are "industry-standard solutions" that "have been the norm now for years").

6 *See, e.g.*, Reply Comments of AdTec, Administrative and Technical Consulting, Inc., WC Docket No. 13-184 (filed Sept. 18, 2019) (relaying exchange from Indiana school technology directors describing student's successful DDoS attack and risk of future attacks).

7 *See, e.g.*, Reply Comments of the Ohio Information Technology Centers at 9-10, WC Docket No. 13-184 (filed Sept. 3, 2019) (explaining that services including "data loss prevention" and

- **Network Traffic Analysis and Behavioral Anomaly Detection** systems use machine learning to automatically establish baseline user and device behavior and detect anomalous activity that may indicate a threat. These tools are particularly important for preventing attacks that exploit vulnerabilities unknown even to vendors (known as "zero-day attacks"), which are not detectable by traditional signature-based systems, and ensuring resilient and secure networks in schools and libraries.[8]

Please be in touch if you have any questions.

Sincerely,

Julie A. Veach
Counsel to Aruba, a Hewlett Packard Enterprise Company

Attachment

cc: Nirali Patel
Kris Monteith
D'wana Terry
Ryan Palmer
Kate Dumouchel
Gabriela Gross
Bryan Boyle
Gavin Logan
Stephanie Minnock
Joe Schlingbaum

"comprehensive encryption of data at rest and on mobile devices" are of "vital importance . . . in protecting student privacy and security, as well as maintaining the availability of the educational resources school networks support" (quoting CoSN Cybersecurity Report at 3)); Comments of the State of South Carolina at 4, WC Docket No. 13-184 (filed Aug. 19, 2019) (explaining that storing data on data servers "can insulate [systems] from ransomware attacks").

[8] *See, e.g.*, Comments of EducationSuperHighway at 7 (explaining that network management systems are necessary to "maintain[] and optimize[] networks" and "ensure both performance and reliability").